Penetration test preparation checklist

BERRY9 IT SERVICES
VAPT and offensive security, Hyderabad
berry9.com

Use this before a web, API, mobile or network penetration test starts. Tick each line, hand the sheet to your tester at the kickoff call, and the days you pay for go into testing instead of waiting for access.

1. Scope

- ☐ Applications, APIs, apps and networks to be tested are listed by name, address and version.
- ☐ The reason for the test is written down: launch, customer request, audit, a recent change or an incident.
- ☐ Environments are chosen: staging that matches production, or production with agreed windows.
- ☐ Exclusions are listed: third-party systems, payment pages you do not own, anything that must not be touched.
- ☐ The test type is agreed: black box, gray box or white box.

2. Access

- ☐ Test accounts exist for every user role, with the logins checked, and an administrator account where needed.
- ☐ Sample data is loaded and is not real customer data.
- ☐ API documentation, an OpenAPI file or a Postman collection is ready.
- ☐ For internal networks: a VPN account, a jump host or a device to place on the network is arranged.
- ☐ For mobile apps: a release build, test devices or permission to use emulators.
- ☐ Single sign-on, one-time passcodes and captchas have a test route that does not block the tester.

3. People and notices

- ☐ One named contact can answer questions during the test, and one emergency number is shared.
- ☐ Your security team, hosting provider, managed service provider and cloud account owner are told the dates.
- ☐ The tester's source addresses are allowed through firewalls, the web application firewall and rate limits.
- ☐ If you want to see whether your defenders notice, that is stated in writing before the test.

4. Safety

- ☐ A backup is taken before testing starts, and a restore has been tried.
- ☐ Major releases and risky changes are paused for the test window.
- ☐ Testing hours are agreed, with quieter windows for heavy checks.
- ☐ Rules of engagement are signed by both sides: scope, exclusions, windows, what may be shown as proof and when to stop and call.
- ☐ Data handling is agreed: where findings are stored, who may see them and when they are deleted.

5. What to have ready, by target

Web applications and APIs

- ☐ Two accounts per role, in two tenants if the product is multi-tenant.
- ☐ List of integrations, webhooks and file uploads.
- ☐ Old API versions and staging hosts identified.

Mobile apps

- ☐ Android and iOS builds of the same version.
- ☐ Backend environment the app talks to.
- ☐ List of third-party SDKs that are out of scope.

Networks and Active Directory

- ☐ External IP ranges and domains, with owners.
- ☐ A standard-user domain account and a network position.
- ☐ Segments, sites and systems that must stay untouched.

Cloud accounts

- ☐ Read-only audit access for each account in scope.
- ☐ Account owners who can answer questions.
- ☐ Production resources excluded from active testing.

6. After the test

- ☐ A readout call is booked for the day the report arrives, with the people who will fix the issues.
- ☐ An owner is named for each finding, and dates are set for critical and high ones.
- ☐ The retest is scheduled, and the shareable summary is ready for customers and auditors.
- ☐ The report, scope and dates are filed together, because auditors and customers will ask for them.

Questions, or want a scope for your systems? Call +91 86868 92922 or write to contact@berry9.com.
Request a scoping call at berry9.com/contact/

Last reviewed
November 2026